MOORE Singhi

BOT MANAGEMENT

"Control Bot traffic to protect yourself from attack"

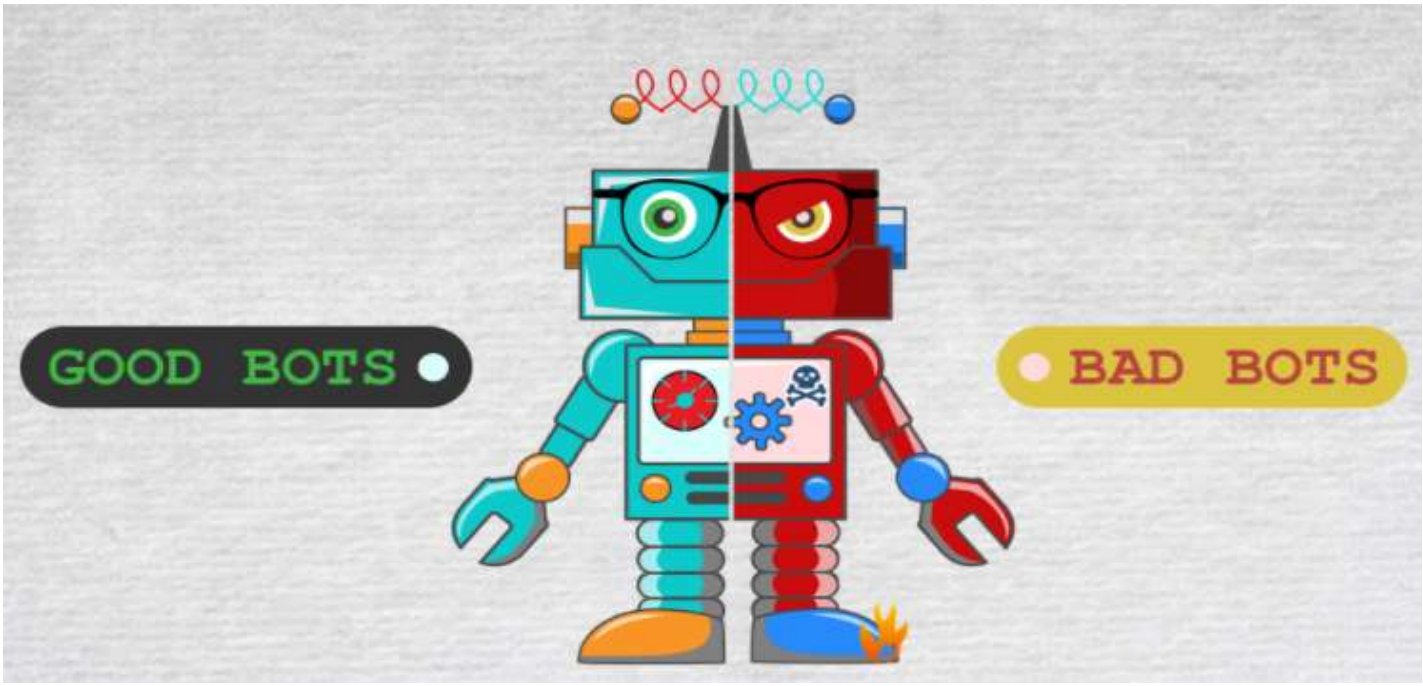
FOREWARD

Currently, lot of discussion is happening around Bots. Whether it is good or bad? How to be careful on Bots? Which are of malicious nature? Let's understand what Bot is all about and how can we protect our organization from its risk, if any.

A bot is a software program which operates on the network and performs programmed repetitive tasks. Some bots over internet are good, whereas other bots can be bad and have a huge negative impact on a websites or applications.

Bots usually interact with webpages, chat with users, or look for attack targets over the network. Some bots are useful, such as search engine bots that index content for search or customer service bots that help users. Other bots are "bad" and are programmed to break into user accounts, scan the web for contact information for sending spam, or perform other malicious activities. If it's connected to the Internet, a bot will have an associated IP address. Bots can be:

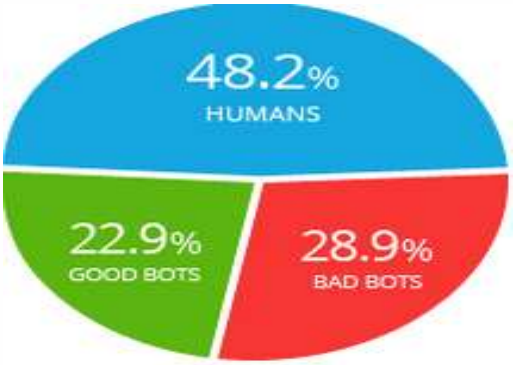
Social media bots: Bots that operate on social media platforms.
Malicious bots: Bots that scrape content, spread spam content, or carry out credential stuffing attacks.
Chatbots: It simulate human conversation by responding to certain phrases with programmed responses.
Googlebots/Web crawlers: These Bots scan content of webpages for personal gain or harm the victims.



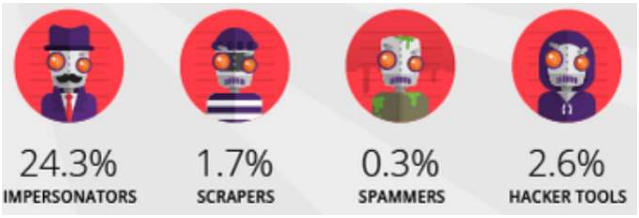
MAJOR BOT ATTACKS RECENTLY

Almost 90% of all websites experienced a bot attack.

The latest data research reveals that, bot traffic accounted for more traffic (50%) than humans where almost 30% accounts for Bad Bots. These are primarily due to the ignorance of users about Bot activities.



A major concern is that bad bots responsible for malicious activity is increasing gradually. Primarily, impersonator bots are most often used to launch DDoS attacks, were the most active, accounting for 24.3% of all traffic on the network



Impersonators

- Bots that falsely pretends other person by bypassing security solutions. Generally used for DDoS attacks.

Scrappers

- Bots used for unauthorised data extractions and the reverse engineering of different models.

Spammers

- Attackers injects spam links into forums, discussion and comment sections to impact victims performance.

Hackers Tools

- Attackers look for sites with vulnerabilities to exploit for data theft, malware injections, etc.

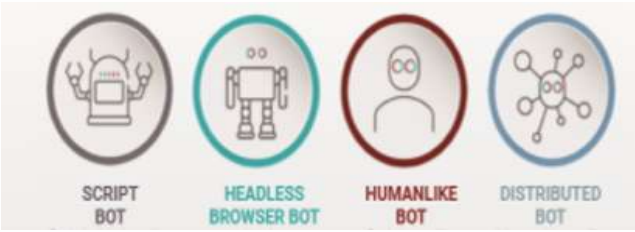
MAJOR MALICIOUS BOT ACTIVITY

Bots that intends to carry out cybercrime, such as spamming, identity theft or account takeover, are "bad" bots. Some of these activities may be illegal as per law, while some may not have to break any laws to be considered malicious.

Malicious bot activity generally includes:

- Stuffing of credentials
- DoS or DDoS attacks
- Brute force attack on passwords
- Inventory hoarding
- Web/content scraping
- Spams
- Email address harvesting
- Click fraud

To carry out above attacks and impersonate the source of the attack traffic, bad bots may be distributed in a botnet, meaning copies of the bot are running on multiple devices, often without the knowledge of the device owners. Because each device has its own IP address, botnet traffic comes from tons of different IP addresses, making it more difficult to identify and block the source of the malicious bot traffic.



- Script Bots - Repititive basic Task Automation
- Headless Browser Bots: Abusing legitimate programs
- Humalike Bots: Humanlike interaction capability
- Distributed Bots: Advanced largescale humannlile interaction capabilities

MOORE Singhi

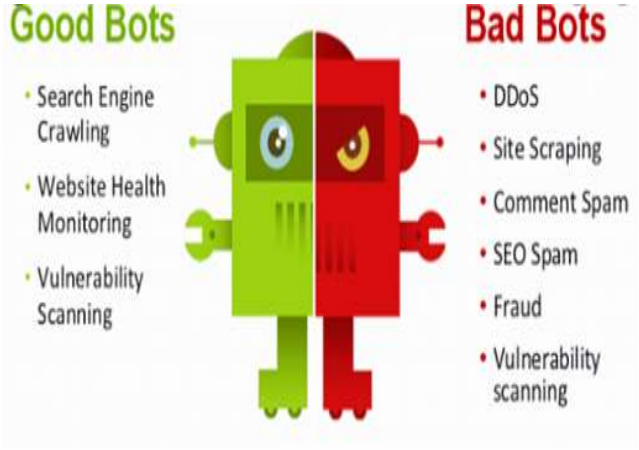
BOT MANAGEMENT

There are various Bot management solution providers who are able to sort out harmful bot activity from user activity and helpful bot activity via machine learning. Various Bot Management solutions stops malicious behavior without impacting the user experience or blocking good bots. Bot management solutions are able to identify and block malicious bots based on behavioral analysis that detects anomalies, and still allow helpful bots to access web properties.

Bot management solutions comes with 'Bot Manager' functionality, which is a software product that manages bots. Bot Managers scans network traffic and block malicious bots and allow good bots, instead of simply blocking all non-human traffic. If all bots are blocked and Google bots aren't able to index a page, for instance, then that page can't show up in Web search results, adversely impacting network traffic to the website.

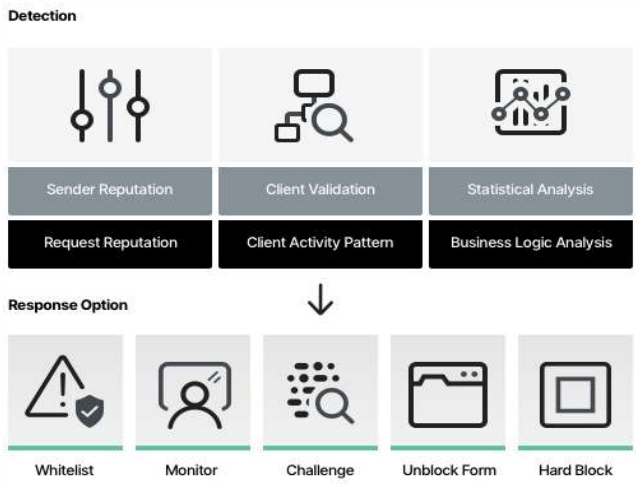
A good Bot Manager accomplishes the following goals. It can:

- Differentiate between bots vs. human visitors
- Locate and track bot reputation
- Identify bot origin IP addresses and block based on IP reputation
- Track and analyze bot behavior
- Identity 'bad' bots vs. 'good' and maintain allow lists for 'good' bots.
- Deny access to certain content or resources for "bad" bots.
- Challenge potential bots via a Captcha test, JavaScript injection, or other methods
- Rate limit any potential bot over-using a service



Response Option of Bot detection

Bots are detected either by carrying out Senders Reputation, Client Validation or Statistical Analysis. A combination of these strategies can further increase the chances of bot detection.



Based on the nature of detection, required Response options need to be selected, which can range from Whitelist (identification of bots and its listing), Bot activity monitoring, challenge activities, unblocking the form or Hard Blocking its services.

SUMMARY

Cyber Criminals are increasing the use of malicious Bots to a great extent now a days and the approach adopted by them are becoming more and more sophisticated. New and latest technologies are being adopted by attackers to attack the organizations.

To combat such attacks, it is becoming critical for organizations to adopt latest Bot security measures, implement Bot Management solutions and get their systems and network audited on a regular basis.

Further, organizations should upgrade themselves to the extent possible and should apply multiple, overlapping, and mutually supportive defensive systems to guard against possible Bot exposures. Organizations should not be in misconception that only high-profile companies in specific industries get attacked. In reality, based on recent study, every organization - big or small, across all industries is a target.

One of the important testing that can be conducted by organization on an annual basis is Vulnerability and Penetration Testing (VAPT) to identify any vulnerability created by Bots in the organization. Such vulnerabilities should be capped with required Bot Management solutions available.

Authored By:

Raj Poddar

CA, CISA, MBA, CEH, CHFI
Partner – IT Consulting
Moore Singhi Advisors LLP

Our Expertise Services

- *Cyber Security Audits*
- *VAPT Assessment*
- *Post Implementation Audit – SAP, Oracle, D365, etc.*
- *Segregation of Duties (SOD) Analysis*
- *ITGC Audits*
- *ERP Process Audits – SAP, Oracle, etc.*
- *Windows Configuration Testing*
- *Secured Network Architecture Review*
- *ISO 27001 Compliance and Audit*
- *GDPR Compliance*
- *NBFC Compliance Audit*
- *IT Policy Documentation and review*
- *SOC 1 & SOC 2 Audits*
- *Digital Forensic Audit*

TOUCH POINTS

Kolkata
161, Sarat Bose Road
Kolkata 700 026
Tel: +91 (33) 2419 6000/1/2
Email- Services@singhico.com

Hyderabad
5-4-187/3 & 4 Soham Mansion
M. G. Road, Secunderabad - 500 003
Tel: +91 (0)40 2754 2635 / 1015

Ahmedabad
705 P B Parekh Tower,
Near Diwan Ballubhai School,
Kankaria
Ahmedabad – 380022
Tel: +91 (0) 79 - 2547 1562
Email: ahmedabad@singhico.com

Mumbai
B2 402B, Marathon Innova, 4th Floor, Off Ganpatrao Kadam Marg
Lower Parel, Mumbai - 400 013
Tel: +91 (0) 22 2495 2881
Email: mumbai@singhico.com

Chennai
Unit-11-D, 11th Floor, Ega Trade Centre,
809, Poonamallee High Road, Kilpauk,
Chennai - 600 010
Tel: +91 (44) 4291 8459
Email: chennai@singhico.com

Bengaluru
No.28, R V Layout, V S Raju road,
Kumara Park West
Bangalore- 560 020
Ph. No.: +91 80 23463462/65
Email: bangalore@singhico.com

Delhi NCR
Unit No.1704, 17th Floor,
World Trade Tower (Tower-B)
DND Fly Way, C-01, Sector 16,
Noida-201301
Tel. No - 0120-2970005, 9205575996
Email- newdelhi@singhico.com

Nagpur
1st Floor, VCA Complex, Civil Lines
Nagpur - 440001
Tel: +91 (0)71 2664 1111
Fax No.: +91 (0)71 2664 1122

DISCLAIMER

Thispublicationcontainsinformationinsummaryformandisthereforeintendedforgeneralguidance of clients / associates and is meant for private circulation only. We shall not accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

This document has been compiled based upon information / documents available in public domain and sources believed to be true and reliable. However, no representation is made that it is accurate and complete.